

Application No. 09/786,756
 Amendment Dated June 13, 2005
 Reply to Office Action of February 11, 2005
 Replacement Specification Sheet

A

B

5

choice g $2 \leq g \leq r-2$

$[g] P = x, y$

$x = \sum x_i t^i \rightarrow i = \sum x_i 2^i$

message M

$c = i \bmod r$

$d = g^{-1} (M + ac) \bmod r$

$M, (c, d) \longrightarrow$

$1 \leq c \leq r-1 ?$ no
yes

error

$1 \leq d \leq r-1 ?$ no
yes

error

$h = d^{-1} \bmod r$

$h_1 = Mh \bmod r$

$h_2 = ch \bmod r$

$T = [h_1] P + [h_2] Q = (x', y')$

|

$T = O ?$ yes

| no

$x' = \sum x_i t^i \rightarrow i' = \sum x_i 2^i$

$c' = i' \bmod r$

$c' = c ?$ no

yes

GOOD

BAD

10